

Appl. No. 10/033,373
Amdt. dated December 5, 2005
Reply to Office Action of October 6, 2005

REMARKS

Claims 1 to 6, 8 and 10 were pending in the application at the time of final examination. Claims 1 to 6, 8 and 10 stand rejected as anticipated.

Claims 1 to 6, 8 and 10 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,453,353, hereinafter referred to as Win. In maintaining the rejection of Claim 1 in the final office action, the rejection did not explain the errors in Applicants' analysis, but rather reduced it to a sentence and then simply restated the conclusions in the rejection citing the same information as in the rejection. Consequently, the final rejection failed to clarify what was considered in the string citations to read on the claims and what the errors were in Applicants' interpretation of those string citations. Applicants respectfully continue to traverse the anticipation rejection of Claim 1.

Claim 1 recites two actions:

enrolling with an authority, said enrolling
creating enrollment results, said enrollment results
comprising user data; and
using said enrollment results to obtain a
service from a service provider, said service
provider capable of communicating with said authority
to verify said enrollment results.

The abstract of Win stated:

The information resources are stored on a protected Web server. A user of a client or browser logs in to the system. A runtime module on the protected server receives the login request and intercepts all other request by the client to use a resource. The runtime module connects to an access server that can determine whether a particular user is authentic and which resources the user is authorized to access. User information is associated with roles and functional groups of an organization to which the user belongs; the roles are associated with access privileges. The access server connects to a registry server that stores information about users, roles,

GUNNISON, McKay A
HODGSON, LLP
Gardens West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(707) 635-0880
Fax (707) 635-0888

Appl. No. 10/033,373
Amdt. dated December 5, 2005
Reply to Office Action of October 6, 2005

functional groups, resources, and associations among them. The access server and registry server exchange encrypted information that authorized the user to use the resource. The user is presented with a customized Web page showing only those resources that the user may access. (Emphasis Added.)

Thus, Win taught that a user logs onto a protected server and provides a request to use a resource. In response, the protected server performs actions to determine that the user is authorized to use the resource and then returns a Web page to the user. The protected server provides the user a customized Web page.

Apparently, the protected server is being cited as the authority of Claim 1. With this construction, apparently, the enrollment results are the customized Web page. The user could use the customized Web page to obtain a service from a service provider using a resource URL in the customized Web page as shown in Fig. 5E and the figure in the Abstract.

However, Win fails to teach that the resource provider associated with the resource is "capable of communicating with said authority to verify said enrollment results," as recited in Claim 1. In fact, such functionality would not be required because the customized Web page provided only authorized links. Accordingly, Win teaches a fundamentally different process from that recited in Claim 1 in the Abstract.

With respect to Figs. 3B and 3C, Applicants first note that Win teaches:

Access Server 106 stores a log-in page, Authentication Client Module and Access Menu Module. The Authentication Client Module authenticates a user by verifying the name and password with the Registry Server 108. If the name and password are correct, the Authentication Client Module reads the user's roles from the Registry Server 108. It then encrypts and sends this information in a "cookie" to the user's browser. (Emphasis Added)

Appl. No. 10/033,373
Amdt. dated December 5, 2005
Reply to Office Action of October 6, 2005

Win, Col. 6, lines 41 to 48.

Specifically, Win taught that an Authentication Client Module authenticates a user and sends a cookie that includes the "user's roles." Thus, the rejection appears to equate "authentication" with enrolling and the cookie as "enrollment results" of Claim 1.

Assuming this is correct, Figs. 3B and 3C show the action of protected server 104, and in particular HTTP server 202 within protected server 104. Win unambiguously taught that HTTP server 202 includes a Runtime Module that "functions to provide a Remote Configuration Service, an Authentication Verification Service, and an Authorization Verification Service." (Win, Col. 7, lines 38 to 41.) Win stated:

. . . Runtime Module 206 calls the Authentication Verification Service to check whether an authenticated user is making the request. An authenticated user is one who has successfully logged into the system. A user is considered authenticated if the request contains a "user cookie" that can be decrypted, and the request's IP address matches that in the cookie. If the conditions are not satisfied, then the user cannot be authenticated, and as shown in state 314, Runtime Module 206 returns a redirection to the Login URL. As shown by state 316, HTTP Server 202 returns the redirection to the Login URL to the browser 100. (Emphasis Added.)

Win, Col. 8, lines 25 to 35.

Thus, the Runtime Module 206 calls the authentication verification service that is executing on protected server 104 as shown in Fig. 2 of Win. Accordingly, protected server 104, which provides the resource requested by the user, does not communicate with access server 106 to verify the results, but rather performs the actions itself.

Thus, Win taught that one entity provided the cookie, access server 106, and a different entity did the verification, protected server 104. Thus, Win fails to teach a "service provider capable of communicating with said authority to verify said enrollment results," as recited in Claim 1. The service

GUNNISON, MCKAY &
RODGSON, LLP.
Gardes West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(415) 625-0180
Fax (415) 625-0888

Appl. No. 10/033,373
Amdt. dated December 5, 2005
Reply to Office Action of October 6, 2005

provider 104 of Win does not communicate with access server 106 to verify the results in the cookie. Moreover, by teaching that protected server 104 performs the authentication using a service of Runtime Module 206, Win teaches away from the service provider of Claim 1. Applicants request reconsideration and withdrawal of the anticipation rejection of Claim 1.

Claims 2, 3, 4, 5, and 8 include a limitation equivalent to that quoted above from Claim 1. Thus, the comments with respect to Claim 1 are applicable to each of Claims 2 to 5 and 8, and are incorporated herein by reference. Applicants request reconsideration and withdrawal of the anticipation rejection of each of Claims 2 to 5 and 8.

In maintaining the anticipation rejection of Claim 6, the rationale for maintaining the rejection simply asserted the statements as used in rejection of the claims. The rationale, for example, did not cite with more specificity what in Win was considered to be the user-controlled secure storage device. The cited section of Win describes a process that results, if successful, in the generation of a cookie. A user does not control a cookie. The browser and not the user selects the cookie that is sent. Accordingly, a cookie fails to teach exactly

means for receiving a user-controlled secure storage device;

Applicants further point out that this is a means plus function element and so must be interpreted as directed in the MPEP, for such elements. Applicants request reconsideration and withdrawal of the anticipation rejection of Claim 6.

Applicants respectfully traverse the anticipation rejection of Claim 10. The rejection cites to Figs. 3B and 3C and Col. 6, lines 58 to 65 of Win, which stated:

GUNNISON, MCKAY &
HODGSON, LLP.
Gardens West Office Plaza
1900 Gardens Road, Suite 220
Menlo Park, CA 94025
(831) 655-0880
Fax (831) 655-0888

Appl. No. 10/033,373

Amdt. dated December 5, 2005

Reply to Office Action of October 6, 2005

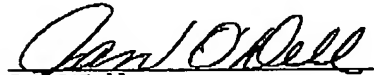
When the user selects a resource, the browser sends an open URL request and cookie to a Protected Web Server. A Protected Web Server is a web server with resources protected by the Runtime Module. The Runtime Module decrypts information in the cookie and uses it to verify that the user is authorized to access the resource. The cookie is also used by the resource to return information that is customized based on the user's name and roles.

The open URL request is at most a service request, and the cookie apparently is being construed as a set of user data. However, Win explicitly teaches that two items, the open URL request and the cookie are used. This fails to teach or suggest "a service request, a first set of user data, and a second set of user data," which are three items. The teaching of two items by Win fails to teach the invention in the same detail as recited in Claim 10. According to the MPEP, as quoted in the prior response and incorporated herein by reference, Win fails to anticipate Claim 10. Applicants request reconsideration and withdrawal of the anticipation rejection of Claim 10.

Claims 1 to 6, 8 and 10 remain in the application. For the foregoing reasons, Applicant(s) respectfully request allowance of all pending claims. If the Examiner has any questions relating to the above, the Examiner is respectfully requested to telephone the undersigned Attorney for Applicant(s).

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being facsimile transmitted to the U.S. Patent and Trademark Office, Fax No. 1-571-273-8300, on December 5, 2005.


Jan O'Dell

December 5, 2005
Date of Signature

Respectfully submitted,



Forrest Gunnison
Attorney for Applicant(s)
Reg. No. 32,899